UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/062,125	01/31/2002	James Kleinsteiber	112-0039US	2526

29855 7590 10/27/2005

WONG, CABELLO, LUTSCH, RUTHERFORD & BRUCCULERI, P.C.
20333 SH 249
SUITE 600
HOUSTON, TX 77070

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/062,125	KLEINSTEIBER ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 August 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-61 and 72-87* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-61 and 72-87* is/are rejected.

7)☐ Claim(s) *1-61,77 and 79-87* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 January 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 8/5/2005.

DETAILED ACTION

Election/Restrictions

Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. *Claims 1-61, and 72-87, drawn to a system for mutually authenticating direct links between network devices, classified in class 713, subclass 201, subject matter further including means or steps for providing system security at network level.*

II. *Claims 62-71 and 88-89, drawn to a method for* mutually authenticating direct *links between network devices including a distributed time service, classified in class 713, subclass 169, subject matter wherein both a transmission and reception entity are determined to be genuine by each other.*

The inventions are distinct, each from the other because of the following reasons:

Inventions I and II are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because the combination does not require distribution of a MAC list to all nodes in the network, distributing a DCC list to all nodes in the network, or a three pass authentication scheme. The subcombination has separate utility such as mutual authentication between ports of devices in a network.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

Applicant's election without traverse of Claims 1-61 and 72-87 in the reply filed on 8/5/2005 is acknowledged.

Claims 1-61 and 72-87 have been examined and claims 62-71 and 88-89 have been cancelled.

Title

The title of the invention is acceptable.

Priority

This application has no priority claimed.

Therefore, the effective filing date for the subject matter defined in the pending claims in this application is 1/31/2002.

Drawings

The drawings filed on 1/31/2002 are acceptable for examination proceedings.

Claim Objections

Claims 1-61 and 77, 79-87are objected to because of the following informalities:

Claim 1 Line 4 should not be capitalized.

Claim 1 Line 9 and Claim 35 Line 6 should recite "a communication media" not "an communication media".

Claim 77 does not contain a period.

Claim 79 contains multiple periods, including 2 in line 11.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-61, 72, and 76-78 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "secure location" in claims 1, 13, is a relative term which renders the claim indefinite. The term "secure location" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. In this particular instance, one of ordinary skill in the art would be unable to determine what constitutes "a secure location". For example, would a fireproof room be considered a secure location. Would a room anchored to the earth be considered a secure location. Would a plaza with armed guards be considered a secure location. As such, one of ordinary skill in the art would not be able to determine the scope of the claim. Therefore, claim 1 is rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

The term "less secure location" in claims 1, 13 is a relative term which renders the claim indefinite. The term " less secure location" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would

not be reasonably apprised of the scope of the invention. In this particular instance, one of ordinary skill in the art would be unable to determine what constitutes "a less secure location". For example, would a non-fireproof room be considered a less secure location. Would a room not anchored to the earth be considered a less secure location. Would a plaza with no armed guards be considered a less secure location. Furthermore, the claim gives no basis as to what the location is less secure than. As such, one of ordinary skill in the art would not be able to determine the scope of the claim. Therefore, claim 1 is rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

The term "substantive" in claims 1, 18, 19, 35, 72, and 76 is a relative term which renders the claim indefinite. The term "substantive" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. In this particular instance, one of ordinary skill in the art would be unable to determine what is considered substantive communication. As such, one of ordinary skill in the art would not be able to determine the scope of the claim. Therefore, claims 1, 18, 19, 35, 72, and 76 are rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

Claim 72 recites the limitation "said devices". There is insufficient antecedent basis for this limitation in the claim.

Claims 2-34, 36-61, and 77-78 are rejected by virtue of their dependency to an above rejected claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-13, 17-19, 35- 47, 51-53, and 72-73 are rejected under 35 U.S.C. 102(b) as being anticipated by Sudama et al. (US Patent Number 5,619,657) hereinafter referred to as Sudama.

Regarding claim 1, Sudama disclosed a method of operating a secure network having plurality of network nodes, each node comprising one or more ports (See Sudama Abstract), the method comprising the steps of: locating one or more nodes in a secure location (See Sudama Fig. 2); locating one or more nodes in a less secure location (See Sudama Col. 8 Paragraph 4); communicating selected management information from a primary configuration node to all other nodes in the secure network (See Sudama Col. 5 Paragraph 3), said communicating having the sub-steps of, a first port on a first node sending said management information to a second port on a second node via an communication media exclusively shared by said first port and said second port (See Sudama Col. 8 Paragraph 4 and Fig. 2); allowing no management access to said secure network from nodes located in said less secure locations (See Sudama Col. 8 Paragraph 4 and Fig. 2); determining a first list of nodes that may send or receive substantive communication in the secure network (See Sudama Col. 5 Paragraph 3); and prior to substantive communication between any two directly-connected ports, authenticating a link between said directly connected ports (See Sudama Col. 5 Paragraph 3).

Regarding claim 35, Sudama disclosed a specific networking node operating in a secure network, said secure network having a plurality of network nodes, each node comprising one or more ports (See Sudama Fig. 2 and Abstract), said specific networking node comprising: a first port on said specific networking node for receiving selected management information from a primary configuration node (See Sudama Col. 5 Paragraph 3 and Fig. 2), said first port directly communicating with a second port on a second node via an communication media exclusively shared by said first port and said second port (See Sudama Fig. 2 and Col. 8 Paragraph 4); a memory for storing (i) management access information (See Sudama Col. 8 Paragraph 1), and (ii) device connection information specifying nodes or ports that may send or receive substantive communication in the secure network (See Sudama Col. 8 Paragraph 1); and a processor for causing the authentication of the link between said first port and said second port prior to substantive communication between said first and second ports (See Sudama Col. 5 Paragraph 3).

Regarding claim 72, Sudama disclosed a method of securing a fabric, said fabric having a plurality of switches all communicatively coupled together, said method comprising the steps of: only allowing communication between pre-defined pairs of said devices as specified by a network operator (See Sudama Col. 5 Paragraph 3); and only allowing substantive communication between devices that are on a pre-defined list of allowed devices (See Sudama Col. 5 Paragraph 3), said pre-defined list stored on a memory in each of said plurality of devices (See Sudama Col. 8 Paragraph 1); and only allowing substantive communication between directly connected ports that have been mutually authenticated (See Sudama Col. 5 Paragraph 3).

Regarding claim 73, Sudama disclosed a network comprising: a plurality of devices including one or more switching and routing devices (See Sudama Col. 5 Paragraph 3), any two of said devices able to inter-communicate only by direct links between each other (See Sudama Fig. 2), all devices able to inter-communicate by forwarding communications through each other (See Sudama Col. 5 Paragraph 3); all of said devices capable of mutually authenticating directly connected links (See Sudama Col. 5 Paragraph 3); one or more pre-designated devices for facilitating management-level control of the network (See Sudama Col. 5 Paragraph 3); and all of said devices carrying a list of all devices allowed on the network (See Sudama Col. 8 Paragraph 1).

Regarding claims 2-12, and 36-46, Sudama disclosed that said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network (See Sudama Col. 5 Paragraph 3), said set of management functions comprising the recognition, operation and succession of primary configuration node (See Sudama Col. 5 Lines 20-21); node connection controls for designating nodes to participate in the secure network (See Sudama Col. 4 Lines 28-31), device connection controls that indicate port relationships in said secure network (See Sudama Col. 5 Lines 22-23), and management access controls that restrict management services to a defined set of endpoints (See Sudama Col. 5 Lines 20-23).

Regarding claims 13, and 47, Sudama disclosed that the step of allowing no management access to said secure network from nodes located in said less secure locations comprises the sub-step of distributing a MAC list to every node in said secure network, said MAC list comprising

an indication of network endpoints from which management access is acceptable (See Sudama Col. 5 Paragraph 3 and Fig. 2).

Regarding claims 17 and 51, Sudama disclosed that the network endpoints comprise uniquely identified nodes resident in said secure network (See Sudama Fig. 2 and Col. 5 Paragraph 3).

Regarding claims 18 and 52, Sudama disclosed that the step of determining a first list of nodes that may send or receive substantive communication in the secure network comprises the sub-step of distributing a DCC list to every node in said secure network, said DCC list comprising definitions that logically bind a port on said primary configuration node to one or more other ports resident in the secure network (See Sudama Col. 5 Paragraph 3 and Col. 8 Paragraph 1 and Fig. 2).

Regarding claims 19 and 53, Sudama disclosed that the step of determining a first list of nodes that may send or receive substantive communication in the secure network comprises the sub-step of distributing a DCC list to every node in said secure network, said DCC list comprising definitions that logically bind each port in said secure network to one or more other ports resident in said network (See Sudama Col. 5 Paragraph 3 and Col. 8 Paragraph 1 and Fig. 2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 14-16, 20-21, and 48-50, and 54-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama. Sudama disclosed distributing a list of management acceptable nodes in a network (See Sudama Col. 5 Paragraph 3), but failed to disclose that the nodes comprise IP addresses, that IP addresses are associated with SNMP or Telnet or HTTP or API, or that the nodes had ports which were uniquely identified by a world wide name. However, it was well known in the art at the time of invention that network nodes have IP addresses, that IP addresses are associated with access from SNMP or Telnet or HTTP or API, and that network ports were uniquely identified by a world wide name. . Therefore, it would have been obvious to the ordinary skill in the art at the time of invention to employ these well known networking features in the network of Sudama.

Claims 22-31, 33-34, 56-61, and 76-87 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama as applied to claim 1 above, and further in view of FIPS PUB 196 ("Entity Authentication Using Public Key Cryptography") hereinafter referred to as FIPS.

Regarding claims 22 and 56, Sudama disclosed mutual authentication performed between the network devices (See Sudama Col. 5 Paragraph 3) but failed to disclose the use of a three pass authentication scheme in order to do so.

FIPS teaches a method for mutual authentication comprising sending a first fact (R_B) from said first port to said second port (See FIPS Section 3.3 Step 2); at said second node, creating a second-type derivative of said first fact (sS_A), sending said second-type derivative of said first fact from said second port to said first port (See FIPS Section 3.3 Step 3); at said first

node, storing said second-type derivative of said first fact in a first memory; sending a second fact (R_A) from said second port to said first port (See FIPS Section 3.3 Step 3); at said first node, creating a first-type derivative of said second fact (sS_B); sending said first-type derivative of said second fact from said first port to said second port (See FIPS Section 3.3 Step 5); at said second node, storing said first-type derivative of said second fact in a second memory; sending defined information concerning said first node (CertB) from said first port to said second port (See FIPS Section 3.3 Step 5); sending a third-type derivative of said defined information concerning said first node from said first port to said second port (It was well known that certificates included signatures of the hash of the certificate); at said second node, comparing said defined information concerning said first node with said third-type derivative of said defined information concerning said first node (It was also well known to verify the signature of the certificate at the receiver); at said second node, comparing said first type derivative of said second fact with said second fact (See FIPS Section 3.3 Step 6); sending defined information concerning said second node (CertA) from said second port to said first port; sending a third-type derivative of said defined information concerning said second node from said second port to said first port (It was well that certificates included signatures of the hash of the certificate); at said first node, comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node (It was also well known to verify the signature of the certificate at the receiver); and at said first node, comparing said second type derivative of said first fact with said first fact (See FIPS Section 3.3 Step 4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of FIPS as the mutual authentication of Sudama. This would

have been obvious because the ordinary person skilled in the art would have been motivated to mutually authenticate the nodes prior to communication between the nodes.

Regarding claim 76, the combination of Sudama and FIPS disclosed a routing device for receiving and directing information in a network (See Sudama Fig. 2), comprising: a public and private key pair (See FIPS Section 3.1.4); one or more ports for coupling to other routing devices and for authenticating said other routing devices and for communicating using said public and private key pair (See Sudama Fig. 2 and Col. 5 Paragraph 3 and the rejection of claim 22 above); a memory for storing a list of all said other routing devices that are allowed to substantively communicate on the network (See Sudama Col. 8 Paragraph 1); and a least one logical management access channel that may be disabled through network management control (See Sudama Col. 8 Paragraph 4).

Regarding claim 79, the combination of Sudama and FIPS disclosed a network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity and (ii) switch connection controls for designating devices to participate in the secure network (See Sudama Col. 5 Paragraph 3), said network configuration entity comprising; a memory for storing an NCE list, said NCE list comprising an indication of each device in the network that may operate as said network configuration entity (See Sudama Col. 5 Paragraph 3); an SCC list, said SCC list comprising an indication of each device allowed to participate in said secure network (See Sudama Col. 5 Paragraph 3); a first secret fact; a first port for sending said secret fact to a second switch; a second port for receiving,

a second-type derivative of said first secret fact from said second switch, pre-defined information about said second switch, and a third-type derivative of said pre-defined information about said second switch; and a processor for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said second switch and said third-type derivative of said pre-defined information about said second switch (See the rejection of claim 22 above).

Regarding claims 23, 33, 58, and 81, the combination of Sudama and FIPS disclosed that the step of comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node, comprises the sub-steps of: reversing the derivation of the third-type derivative of said defined information concerning said second node; and comparing the result of said reversal with said defined information concerning said second node (It was well known at the time of invention that a signature was decrypted using the public key of the certificate authority and compared with the signed data to verify the signature).

Regarding claims 24, 59, and 82, the combination of Sudama and FIPS disclosed that the step of comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node, comprises the sub-steps of: making a third-type derivative of said defined information concerning said second node; and comparing the made third-type derivative with the received third-type derivative (It was well known at the time of invention that a signed hash was decrypted using the public key of the certificate authority and compared with the hash of the certificate to verify the signature).

Regarding claim 25-27, the combination of Sudama and FIPS disclosed that the step, at said second node, of creating a second-type derivative of said first fact comprises the sub-steps of: encoding said first fact to yield an encoded first fact; and encrypting said encoded first fact (It was well known at the time of invention that a signature was created by hashing the data to be signed and then encrypting the hash with a private key of a public key pair).

Regarding claims 28-29, and 85, the combination of Sudama and FIPS disclosed that defined information concerning said first node comprises encryption key information and that encryption key information comprises a public key uniquely associated with said first node (See FIPS Section 3.1.4).

Regarding claims 30-31, 34, 61, and 84, the combination of Sudama and FIPS disclosed that the third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority associated with said first node and said second node (See FIPS Section 3.1.4).

Regarding claims 57, and 80, Sudama and FIPS disclosed that the third port and the fourth port are the same port (See Sudama Fig. 2).

Regarding claim 60, Sudama and FIPS disclosed that the second-type derivative is associated with the third node (See FIPS Section 3.3 Step 3).

Regarding claim 77, Sudama and FIPS disclosed that the certificate authority for the public and private key pair is not the entity controlling management access to said routing device (See FIPS Section 3.1.4).

Regarding claim 78, Sudama and FIPS disclosed a memory for storing distributed time service information (It was well known in the art for network devices to contain network time service information).

Regarding claim 83, Sudama and FIPS disclosed that the second-type derivative is associated with said second switch (See FIPS Section 3.3).

Regarding claims 86-87, Sudama and FIPS disclosed that the first secret fact is a random nonce (See FIPS Section 3.3).

Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama and FIPS as applied to claim 30 above, and further in view of Fischer (US Patent Number 5,422,953).

Sudama and FIPS disclosed the use of certificates (See the rejection of claim 22 above), but failed to disclose the certificate being issued by the manufacturer of the node devices.

Fischer teaches that a manufacturer of a device can also be the issuer of the devices public key certificate (See Fischer Col. 6 Paragraph 3).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Fischer in the network system of Sudama and FIPS by having the manufacturer of the network devices issue the certificates to the devices. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide assurance through the certificate that network device was secure.

Claim 74 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama as applied to claim 73 above, and further in view of Thapar et al. (US Patent Number 5,694,615) hereinafter referred to as Thapar.

Sudama disclosed a network of routers (See Sudama Fig. 2), but failed to disclose the system being used in a fibre channel.

Thapar teaches that the fibre channel addresses the need for very fast data transfers (See Thapar Col. 1 Lines 18-26).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Thapar in the communication network of Sudama by replacing the routers of Thapar with Fibre Channel routers. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow for very fast transfers of large volumes of data.

Claim 75 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama as applied to claim 73 above, and further in view of applicant admitted prior art.

Sudama disclosed a network of routers (See Sudama Fig. 2), but failed to disclose the routers being in locked rooms.

Applicants admitted on page 2 paragraph 2 of the specification that the prior art secured computer equipment by locking it in a room.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of the applicants' admitted prior art in the networking system of Sudama by locking the management devices in rooms. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the devices against tampering and theft.

Conclusion

Claims 1-61 and 72-87 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Schneier ("Applied Cryptography") disclosed methods for verifying certificates and digital signatures.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Matthew Henning
Assistant Examiner
Art Unit 2131
10/24/2005